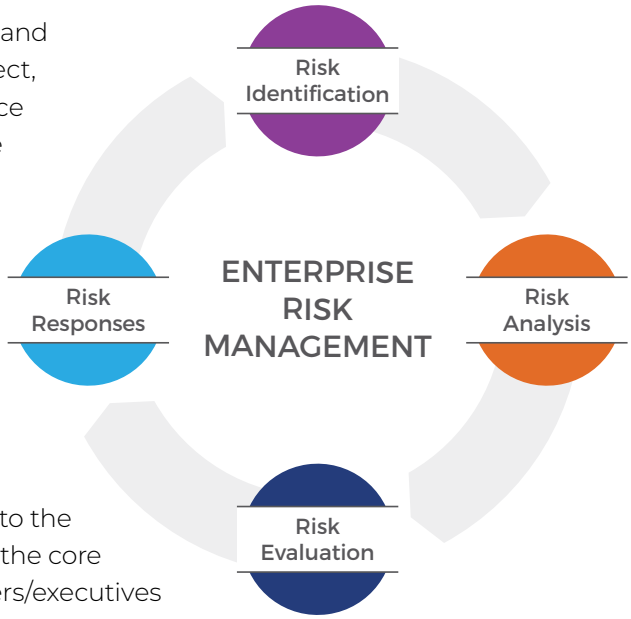
Improve Your Smart Device Security Posture

A CISO's Guide to Enterprise Risk Management for IoT

INTRODUCTION

Governance in cybersecurity describes the policies and processes which determine how organizations detect, prevent, and respond to cyber incidents. Governance often details What must be done to create a secure engineering environment, but attention is needed to the broader question of How to achieve it in the modern organization filled with smart devices. The NIST special publication 800-39 is often used as a basic standard for managing information security risk, but even there the language specifies that the guidelines are voluntary for non-federal organizations, and should be considered only part of a larger enterprise risk management (ERM) program. Security risk related to the operation and use of information systems is one of the core components of organizational risk that senior leaders/executives need to address as part of their risk management responsibilities.



In many organizations, there is a division between governance and management. However, the modern CISO needs to have a clear assignment of risk management responsibility which is shared with their senior leaders and executives — and this mandates a requirement that the CISO understand fully the modern risks of the Internet of Things (IoT) devices at work in their enterprise. The truth is that any object with a sensing interface such as Bluetooth combined with network access can represent a risk to the enterprise.

> The truth is that any object with a sensing interface such as Bluetooth combined with network access can represent a risk to the enterprise

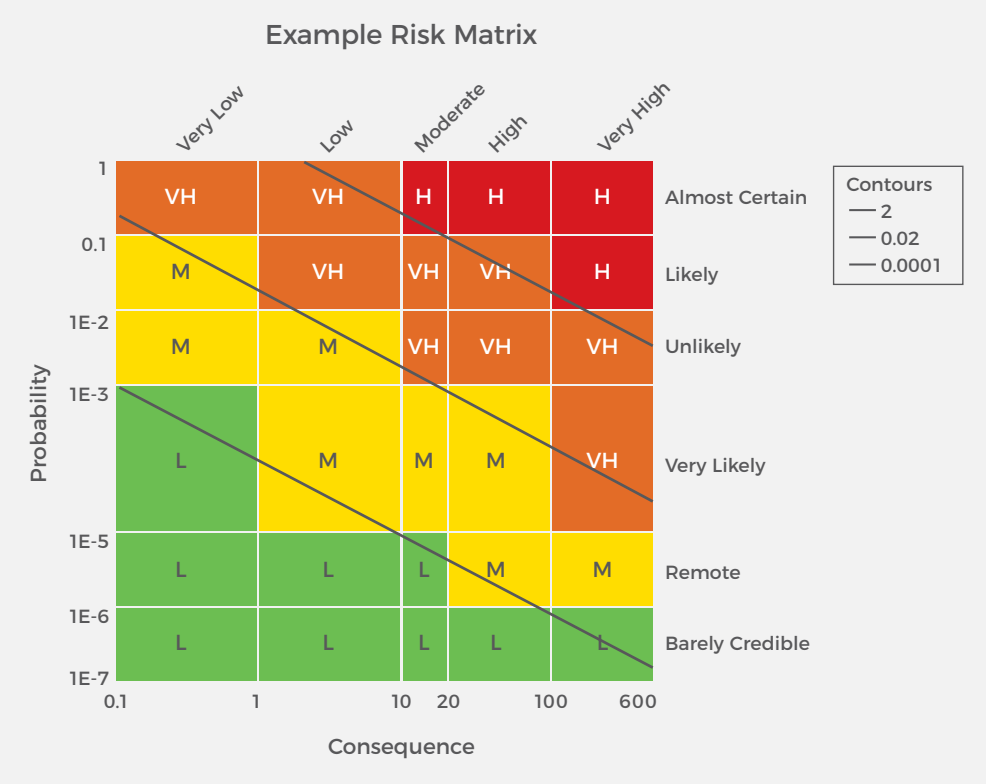
In the past few years, the spread of news stories about attack ingress through HVAC systems, CCTV systems, or even decorative modules like Fish Tanks require a new standard for recognizing risk, the tools to assess the risk and your risk tolerance levels, as well as controlling or mitigating future risk as the environment changes. An organization needs the ability to detect new IoT threats and classify their capabilities, prioritize those threats by their capacity to do harm to the greater information system, and control the threats in a proactive fashion.

RISK ASSESSMENT AND CONFIDENCE

Basic risk assessment is something we all perform daily on any number of environments, where we determine the likelihood of an activity and weigh it against the likelihood of it occurring. It's fairly simple to assign a high risk to an email server (or service) as a standard and well-known source of threats from phishing scams to infected files and malicious URLs. Generally, the executives or operations will put together a list of known risks and weigh against likelihood.

For new organizations or expanding enterprises, this process can start with physical security risks for scouting safe locations to build vs crime rates, weather or geologic concerns, etc. It moves on through sourcing reliably through secure vendors, using reliable businesses and partnerships — all this before we even reach securing engineering systems, network environments, and personnel. A CISO is concerned with managing risk from contractors and new employees through compliance and governance with everything in between — and that includes constant risk assessments which are best achieved through scoring and assessments which are frequent enough to be meaningful as new people and smart devices move in and out of an organization.

Confidence in simple endpoint risk assessments can be easily validated via antivirus and endpoint protection software. Network risk is reduced by intrusion detection systems and monitoring, along with frequent testing for business continuity and disaster recovery. In terms of funding, security and risk investments tend to be in the high range first, and rightly so, followed by settling in both manpower and new software as risk tolerance and experience permit.



The core of good information security risk assessment discipline requires good information about threats, issues, and changing conditions. It's important for good security hygiene that risk scoring gets input from a number of sources from current IT threats, government CERT agencies, and even

> The core of good information security risk assessment discipline requires good information about threats, issues, and changing conditions.

commercial threat feeds containing known malicious URL and IP lists for automatic blacklisting along the network. All of these are the basics and standards of information security, from the perspective of risk assessment and vulnerability management.

The challenge of good risk analysis lies not just in having the right threat sources for external threats, but in evaluating internal dynamic risk as people and smart devices move across locations. The truth is, many smart devices from audio-visual equipment to simple environmental controls were designed for core operation and function rather than considerations of inherent security.

WootCloud helps enterprises look at all smart devices that live or travel into your enterprise with an eye to controlling these devices according to the ISO machinery standard three limits: Use, Space, and Time.

- The Limit of Use describes the normal use of the device, and who is using it.
- The Limit of Space describes the physical location of the device, if it has one, and it's range of expected movements.
- The Limit of Time describes expected life cycle, the need for updates, and more.

> The challenge of good risk analysis lies not just in having the right threat sources for external threats, but in evaluating internal dynamic risk as people and smart devices move across locations.

We bring these up because these are all important informational considerations for the smart devices that move in and through your environment. Smart devices remain a persistent gap in the common risk scoring methodologies of IT and information/data security due to an historic inability to identify, monitor, and control these devices by identifying all the factors of their limits.

RISK SCORES FOR SMART DEVICES

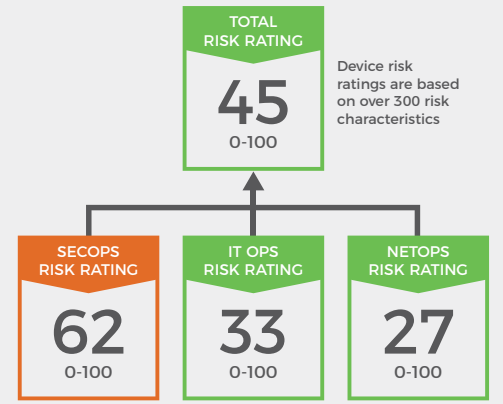
Like all factors of a persistent Risk Management discipline, the risk score of smart devices must be a part of overall risk strategy. WootCloud helps you plan for the Known Unknowns of all types of IoT devices that may have been escaped detection using traditional security gear.

Having a risk score associated with both the known and unknown sensing devices in your environment is invaluable in protecting your organization from a wide variety of Bluetooth hacks and unexpected network attack ingress. WootCloud's risk scoring looks at the following important limits of smart devices including:

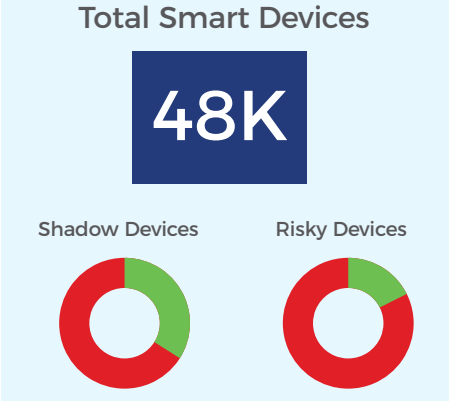
- Managed vs Unmanaged devices
- Static or automated devices with network access
- Unpatched devices, or devices without up-to-date definitions
- Sanctioned vs Unsanctioned access points and hot spots
- Active malware
- Alerts not blocked by firewalls
- Usernames on the device

Having a risk score associated with both the known and unknown sensing devices in your environment is invaluable in protecting your organization from a wide variety of Bluetooth hacks and unexpected network attack ingress.

Your Organizational Device Risk Rating (DRR)



Devices & Risk



Device Profile

By Type		By OS		By Compliance Posture	
Computer	720	Windows	480	Computer	720
Smart Phone	600	iOS	400	Smart Phone	600
Laptop	50	MacOS	221	Laptop	50
Tablet	39	Android	110	Tablet	39
Other	22	Other	100	Other	22

INTRODUCING WOOTCLOUD'S DEVICE RISK SCORE

WootCloud uses traditional risk analysis techniques for network security in a new way; Specifically our device risk score is a combination of static and dynamic factors which make up a smart device's security and risk posture. Our Risk scoring is made up of a proprietary combination of factors that give you immediate response options for security automation as well as post-incident investigation.

Device risk score is represented as a simple equation:

> Score = Likelihood (represented by actual activity) x Impact (Active Data represented by threat severity + Static Data represented by HyperContext device fingerprinting)

Threat Severity — WootCloud uses CVSS-type evaluation of threat types such as Elevation of Privilege, Remote Code Execution, etc. These are constants for the type of attack that smart devices are vulnerable to. WootCloud Threat categories include, but are not limited to:

- Users perform actions that enable future attacks
- Attackers compromise unauthorized device
- Attackers compromise unauthorized or prohibited software
- Attackers exploit known software vulnerabilities

- Attacker launches insider attacks
- Attacker steals credentials and exploits weak authentication
- Attacker exploits account and physical access privileges
- Attackers penetrate network boundaries in either direction
- Attackers gain knowledge about the network
- Weak IT compliance enable attacks
- Weak asset management practices
- Weak Network configurations enable attacks

Static Data — This includes information about the device fingerprinting, i.e. patching status, presence of vulnerabilities such as viruses, multiple user names associated with one device and more. Static data is updated with new vendor patches and known CVE releases.

Active Data — This includes the behavior of the device. It is recognized through many factors such as movement identified by sensors, virtual lateral movement on the network, sudden unexpected activity (e.g. a fish tank on the network suddenly sending SMTP messages to an external address), detection of Emerging Threats, and more.

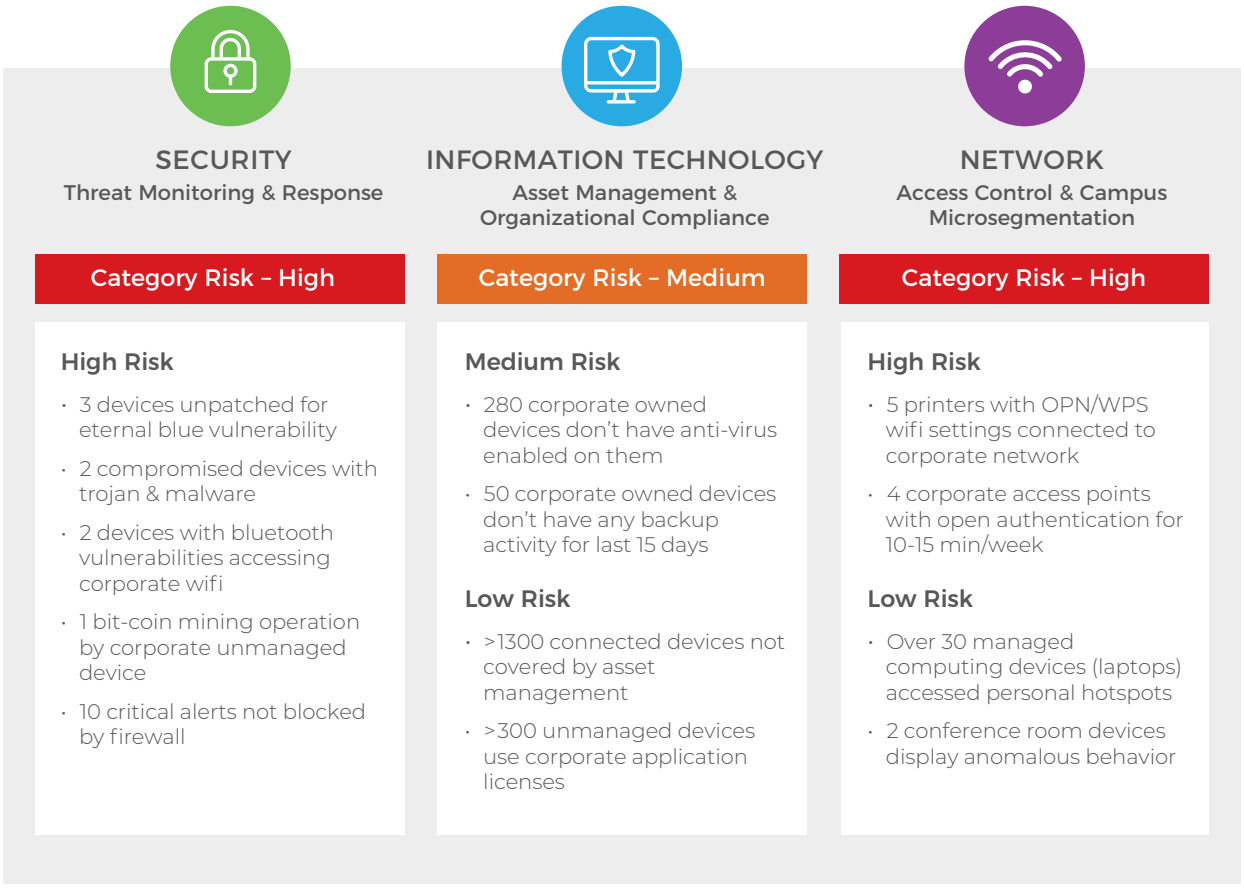
These factors add together more dynamically than many standard risk assessments. If a manager's iPad suddenly visits a building they shouldn't be able to access, or connects to a Finance network share inappropriately, the risk score will go up dramatically as the Likelihood of threat increases. Ditto if a known vulnerability resides on an unmanaged device, and the user appears after hours and logs into infrastructure they are not normally provisioned for.

Finally, it's not enough to tell you your risk Score and expect everyone to understand the fix. WootCloud's executive summaries not only can identify risky devices and user behaviors, they also suggest how to mitigate the threat or plan for contingencies.

RISK SCORES BY ORGANIZATIONAL FUNCTION

Different parts of an organization may involve different risk ratings to represent their core function and governance, and the risk scores should support them. For example, IT Operations has a concern for managed versus unmanaged devices, as well as keeping track of which managed devices need patching. Many static security factors are a concern and the remedy of IT Ops. ITOps will look at some user patterns such as standard user behavior, for instance a sudden change in after-hours work, check in, etc.

NetOps concerns itself heavily with network sanitation such as unauthorized access points, especially in a WiFi enabled environment or LAN. If it touches the network, it needs to be secure. Network Operations looks at behavior in motion, checking for sudden changes SMTP traffic, data loss prevention, and more.



Security Operation needs risk scoring to write rules for controls. Whether you have a data loss prevention solution or run on firewalls and web application control software, knowing the risk of a device affords automation of security measures such as dropping access. User anomalies, behavior anomalies, inappropriate accesses are all factors that should automate into security controls, and be available for incident response as well as forensic investigation.

DevOps need to know when something is amiss with testing, as well as securing intellectual property and source code. Locking down their environment to a strict set of users and devices is key to protecting the IP of the company and reducing organizational as well as business risk.

CONCLUSION

No network is impenetrable, because thanks to mobility and smart devices the components of that network are always in a state of flux. This is why the business of Risk Posture evaluation will always flourish, and CISOs will always have a key role to play within the organization in terms of determining strategy and the tools to keep an organization safe.

No network is impenetrable, because thanks to mobility and smart devices the components of that network are always in a state of flux.

As smart hackers move to compromise smart devices, it's imperative that the risk score of any organization includes a thorough IoT evaluation, including current intelligence on the

> Finally, a centralized risk score for IoT and smart devices allow you to automate security controls, and conduct post-incident review for process improvement.

active devices within the environment to active controls and blocking should the behavior of those devices prove anomalous or suspicious. Any risk management strategy that doesn't include smart devices and a full wireless access management control point is leaving themselves open to attack as well as the exfiltration of data — and may someday be another headline for IT and Security departments to learn from.

Device discovery and fingerprinting, risk scoring those devices, and behavior analytics are the simplest path to getting a handle on risk evaluation for this historically un-checked and unmeasured part of your IT stack and environment. And as time moves on and manufacturers push out security updates, it's important to know how quickly your own team is responding to them.

Finally, a centralized risk score for IoT and smart devices allow you to automate security controls, and conduct post-incident review for process improvement. The business of risk management is dynamic, and WootCloud wants to be your partner for making sure your unseen perimeter is as secure as your firewalls.

NEXT STEPS

Request a WootCloud HyperContext demo

Request a free WootCloud Smart Device Risk Assessment

About WootCloud

WootCloud is the only smart device security platform that uncovers unmanaged devices on both the radio and network spectrum, and analyzes over 300 device parameters to generate device risk scores. This helps organizations discover gaps in their device risk posture and the opportunity to close these gaps. A privately held company, WootCloud is headquartered in San Jose, California, with offices in India and Argentina.

WootCloud HYPERCONTEXT

3031 Tisch Way
Suite 308
San Jose, CA 95128
T: 408-564-4220
sales@wootcloud.com